CATEGORIZE STEP – TIPS AND TECHNIQUES FOR SYSTEMS

NIST RISK MANAGEMENT FRAMEWORK

Security categorization is the most important step in the Risk Management Framework (RMF) since it ties the information system's security activities to the organization's mission/business priorities. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines requirements for categorizing information and information systems. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance in assessing the criticality and sensitivity of the information and associated information system to determine the system's security category (i.e., potential worst case impact from loss of confidentiality, integrity, and availability) and overall impact level.

The system's impact level is used to select a baseline set of security controls for the information system from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, that is then tailored to better reflect the information system's unique circumstances. In addition, the system's impact level determines the rigor applied to the remaining steps in the Risk Management Framework, including the assessment of security controls.

Security categorizations should be reviewed on an ongoing basis to help ensure that they continue to reflect the current organizational priorities and operational environments. The information owner/information system owner is responsible for categorizing the information system.

NOTE: These *Tips and Techniques for Systems* are provided as one example of how NIST SP 800-60 may be implemented to categorize federal information and information systems in accordance with FIPS 199. Readers should understand that other implementations may be used to support their particular circumstances.

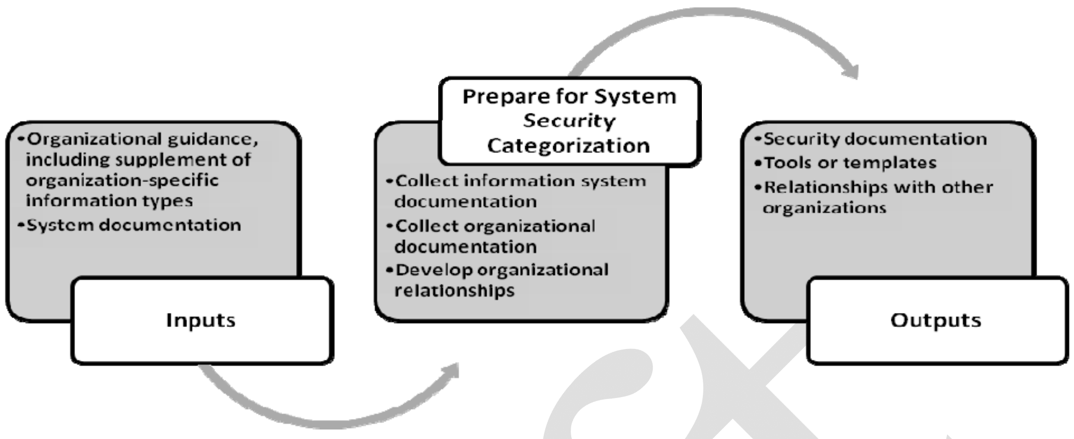
NIST SP 800-60 defines a four-step process for categorizing information and information systems as (i) identify information types, (ii) select provisional impact levels for the information types, (iii) review provisional impact levels and adjust/finalize information impact levels for the information types, and (iv) assign a system security category and overall impact level.

The tips and techniques in this document elaborate on the basic steps and guidance in NIST SP 800-60 as examples for stimulating ideas in implementing categorization standards and guidelines in organization-specific and information system-specific environments.

The ideas and examples for implementing NIST SP 800-60 presented include the following: (i) preparing for security categorizations, (ii) identifying and matching data elements to information types, (iii) defining and documenting information type categorizations, (iv) defining and documenting information system categorization, (v) defining and documenting system overall impact level, (vi) approval for system security category and overall impact level, and (vii) maintaining the system security category and impact level.

PREPARE FOR SYSTEM SECURITY CATEGORIZATION

In order to determine the system security category, the information owner/information system owner collects relevant documentation specific to the information system such as the system description and architecture. In addition, the information owner/information system owner also collects any available guidance documentation issued by the organization. The information owner/information system owner establishes (or maintains) working relationships with others within the organization who are also impacted by the categorization decision (e.g., the information security program office, the enterprise architecture group, information sharing partners).


•Organizational guidance, including supplement of organization-specific information types
•System documentation
Inputs
Prepare for System Security Categorization
•Collect information system documentation
•Collect organizational documentation
•Develop organizational relationships
•Security documentation
•Tools or templates
•Relationships with other organizations
Outputs

Collect Information System Documentation

Prior to categorizing an information system, the information owner/information system owner collects available documentation on the information system. While the details of a new information system may not be known, sufficient information should be available to begin to identify the types of information that will be processed, stored, or transmitted by the system (e.g., system description, concept of operations), typically documented in the initial system security plan. For legacy information systems that are already operating, the information owner/information system owner collects documents that were developed throughout the system development life cycle. These documents could include the data dictionary, database schemas, data requirements documents, samples of system reports and input forms, or software code.

Collect Organizational Documentation

Information owners/information system owners also obtain organization-specific guidance on how to categorize their information systems. Organizations may have guidance that elaborates on the NIST standards and guidance and that provides details on how to categorize their information systems, including organization-specific tools, templates, or checklists to support the categorization process. The organization-specific guidance typically includes internal requirements for reporting and approving the security categories and system's impact level.

Organizations should also identify their unique information types. While NIST SP 800-60, Volume II, includes a comprehensive catalog of information types, the organization may have specific information types representing their unique lines of business that do not map to the information types defined in NIST SP 800-60. The organization may identify their unique information types in a supplement to NIST SP 800-60 of additional, organization-specific information types and make it available to all information owners.

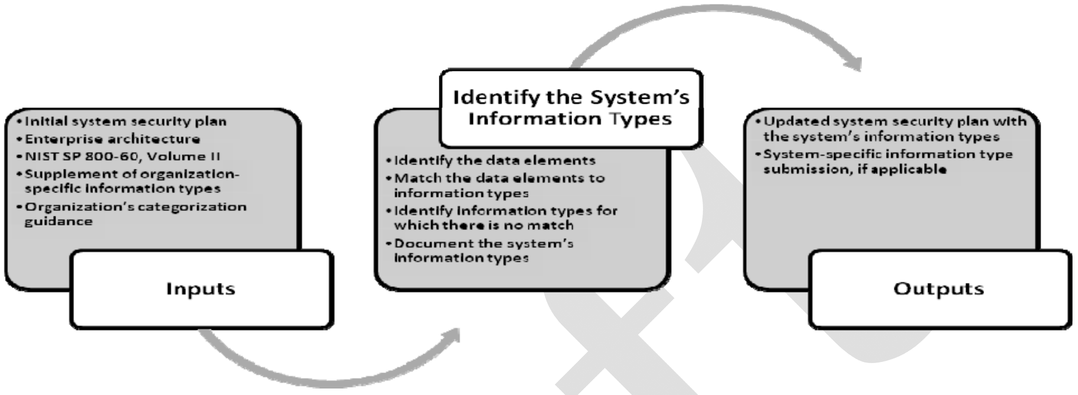
Establish Organizational Relationships

In addition to gathering documentation, information owners/information system owners develop relationships with others within their organization. The information security program office establishes the organization-specific policies on categorizing information and provides any available tools, templates, or checklists to assist with the categorization process. This office is the primary contact for advice and support while categorizing individual information systems.

The information owner/information system owner works with others within the organization including the enterprise architecture group, information sharing partners, and technical operations personnel. Each of these groups can help provide the information needed to effectively categorize an information system.

IDENTIFY THE SYSTEM'S INFORMATION TYPES

The information owner/information system owner identifies the types of information that are processed by, stored in, or transmitted by the information system and documents them in the system security plan. Any information types not included in NIST SP 800-60 or the organization's supplement to NIST SP 800-60 are identified and documented.



Inputs

- Initial system security plan
- Enterprise architecture
- NIST SP 800-60, Volume II
- Supplement of organization-specific information types
- Organization's categorization guidance

Identify the System's Information Types

- Identify the data elements
- Match the data elements to information types
- Identify information types for which there is no match
- Document the system's information types

Outputs

- Updated system security plan with the system's information types
- System-specific information type submission, if applicable

Verify the System Characteristics

The information owner/information system owner verifies the characteristics of the information system and the information processed, stored, or transmitted by the system. This information is typically included in a description of the information system boundary. If the information system boundary has not yet been defined, the information owner/information system owner works with the documentation available and interviews people knowledgeable about the system and its characteristics to define the initial system boundary. This information may be found in various types of documentation including development documents (e.g., solicitation documents, functional specifications, network architecture diagrams), system security documentation (e.g., system security plan, risk assessment, or plans of action and milestones), operational documentation (e.g., rules of behavior or users guides), or training documentation.

The information owner/information system owner obtains as much information as possible on the: (i) purpose of the information system; (ii) organization's mission, lines of business, or resource management functions that the system supports; (iii) system boundary; (iv) the functions, processes, and activities performed by the system; (v) types of users; (vi) individuals, organizations, or systems that share information; (vii) operational environment; and (viii) applications supported by the system and the information that it processes, stores, creates, transfers, or deletes.

Identify Data Elements

Data elements are the smallest unit of information that can be understood. For example, a person's name usually has the following data elements: last name, first name, middle initial, and suffix. Individuals working with an information system are usually more familiar with the data elements than the information types defined in NIST SP 800-60. Identifying the data elements can help to identify the information types. Each information type may include one or more data element.

In addition to identifying each data element, it is necessary to identify how the data elements are used. For example, the data elements for a person's name can be used by a payroll application to issue pay checks. The same data elements may be used in an inventory application to track computer assets assigned to an employee. Therefore, the context in which the data elements are used is relevant when determining the information type.

After the data elements have been identified, they are logically grouped together. The information owner/information system owner prepares a description of each data element group processed by the information system. This description is used to match the data elements in the system with the information types defined in NIST SP 800-60 and the organization's supplement to NIST SP 800-60.

Match the Data Elements to Information Types

Using the descriptions of the data elements or groups of data elements processed by the system, the information owner/information system owner reviews the organization's supplement to NIST SP 800-60 and NIST SP 800-60, Volume II, and match the descriptions to the predefined, approved information types.

In some cases the information type will be very apparent. If an information system is used to develop the budget and determine priorities for future spending, then the data element is clearly the Budget Formulation Information Type. In other cases, the information type will not be very apparent and the information owner/information system owner may need to match the kind of information to a portion of the information type description or an extension of the information type description. For example, information related to processing patent applications may have no obvious match to the information types defined in NIST SP 800-60, Volume II, but can be matched to the protection of intellectual property in the Scientific and Technological Research and Innovation Information Type.

In some cases there is more than one option when matching the data elements to the defined information types. To determine which information type is most relevant to the data element, the information owner/information system owner considers the context in which the information is used. For example, a person's name (with data elements last name, first name, middle initial, and suffix) could be used in a variety of information types. How the person's name is being used in the specific application determines which information type is the best match for the data elements identified in the information system.

NIST SP 800-60, Appendix C, includes management and support function information. Support functions to conduct the government's business include debt collection, customer services, or rule publication information. Management functions that support all areas of the government's business include financial management, human resources, or information and technology management. NIST SP 800-60, Appendix D, includes mission-based information and the mechanisms that the government uses to achieve its goals such as border and transportation security, energy supply, or air transportation information. Since each organization's mission varies, only specific parts of Appendix D will apply to an organization.

In addition to the NIST SP 800-60 appendices, the organization should have a supplement to NIST SP 800-60 of additional, organization-specific information types. The supplement should include information types that apply to the organization and are not included in NIST SP 800-60. The supplement should also identify which mission-based information types from NIST SP 800-60 do not apply to the organization and any organizational adjustments to the provisional impact values.

Identify Information Types for which there are No Matches

In some cases, a particular data element or group of data elements may not be able to be matched to an information type in the organization's supplement to NIST SP 800-60 or in NIST SP 800-60, Volume II. This unique kind of information should be described and an initial security category determined based on the FIPS 199 categorization criteria. The description for the unique information type should include the similar information found in NIST SP 800-60, Volume II: (i) brief title and description of the information type; (ii) recommended security category; and (iii) for each security objective (confidentiality, integrity, and availability) a discussion of the recommended security impact value and the special factors affecting the impact value determination. The description of the unique information type should be submitted to the information security program office for approval and possible inclusion in the organization's supplement to NIST SP 800-60.

Document the System's Information Types

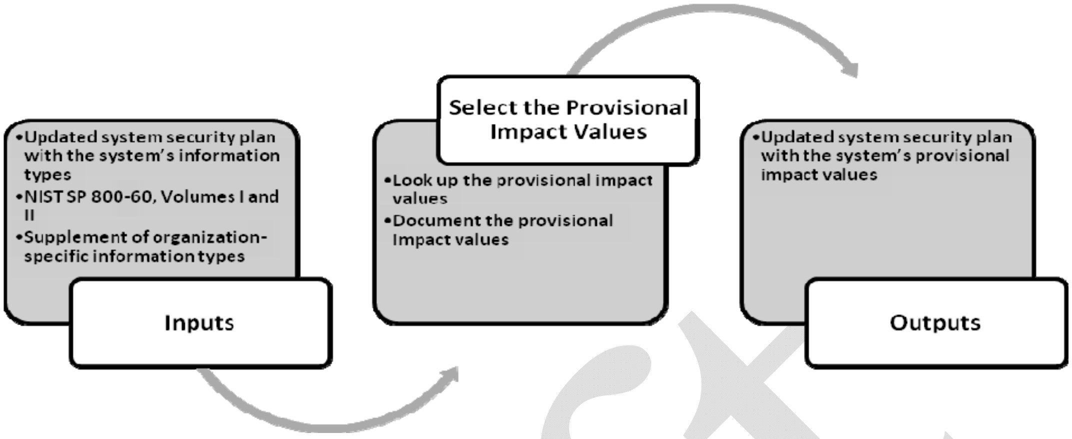
After a system's information types have been identified, they should be documented in the system security plan. A table like the one below provides a convenient way to record all the information needed to support the categorization decision.[1] First, the information types are identified and added to the table. As the categorization process continues, additional information is added to the table. The information on the information types should include the information type title and reference number (from NIST SP 800-60 or the organization's supplement to NIST SP 800-60) and a brief description of the information type. In the example below, a compliance tracking information system is used by the organization to monitor the organization's low- and moderate-impact information systems.

Information Type Title, Reference, Description	Security Category						Adjustment Rationale
	Provisional			Final			
	C	I	A	C	I	A	
Corrective Action, C.2.1.1, POAMs include information on non-compliant information systems within the organization							
Program Evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)							
Program Monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)							
Inventory Control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections							
Provisional System Security Category			[redacted]				
Adjusted System Security Category			[redacted]				
Information System Security Impact Level							[redacted]

SELECT THE PROVISIONAL IMPACT VALUES FOR EACH INFORMATION TYPE

The information owner/information system owner reviews NIST SP 800-60, Volume II, and the organization's supplement to NIST SP 800-60 to determine the provisional, or initial, impact values established for each information type. Regardless of the source of the information type, the provisional impact values for each information type is documented in the system security plan.

[1] This table is a sample method used to record the decisions made during the categorization process. It is not a mandatory format. Organizations may develop their own unique template that captures the information consistent with the requirements in NIST SP 800-60.


•Updated system security plan with the system's information types
•NIST SP 800-60, Volumes I and II
•Supplement of organization-specific information types
Inputs
Select the Provisional Impact Values
•Look up the provisional impact values
•Document the provisional Impact values
•Updated system security plan with the system's provisional impact values
Outputs

Look up the Provisional Impact Values

After the information types have been identified and documented in the system security plan, the provisional impact values for each information type can be determined. Each information type is located in either the organization's supplement to NIST SP 800-60 or NIST SP 800-60, Volume II, Appendices C or D. The provisional impact values are *low*, *moderate*, or *high*. Confidentiality can also have an impact value of *not applicable* when the information type contains public information.

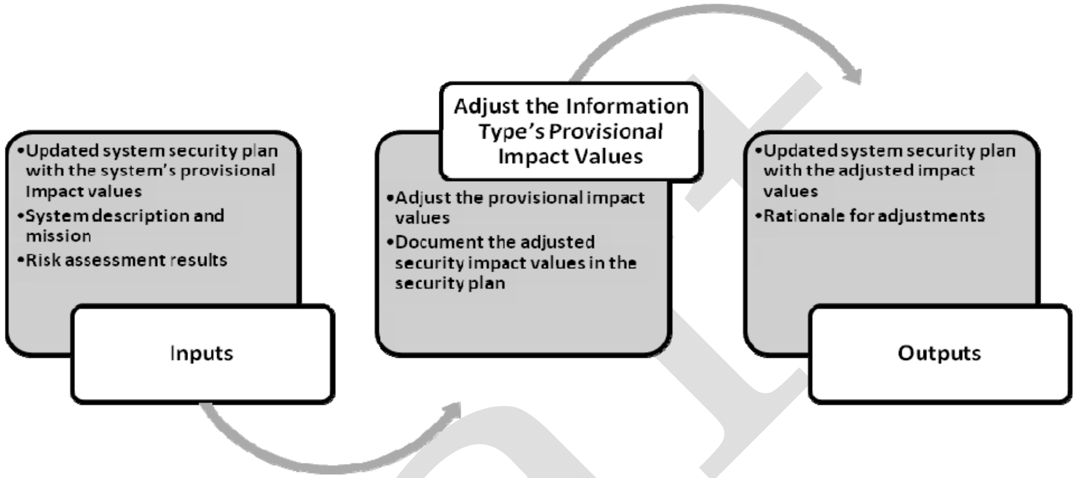
Document the Provisional Impact Values

After the provisional impact values have been identified using the appropriate source document (NIST SP 800-60 or the organization's supplement to NIST SP 800-60), the provisional impact values (low, moderate, high, or not applicable) for each security objective (confidentiality, integrity, and availability) should be added to the chart in the system security plan. For example, the provisional impact values for each of the four previously identified information types have been added to the table.

Information Type Title, Reference, Description	Security Category						Adjustment Rationale
	Provisional			Final			
	C	I	A	C	I	A	
Corrective Action, C.2.1.1, POAMs include information on non-compliant information systems within the organization	L	L	L				
Program Evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)	L	L	L				
Program Monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)	L	L	L				
Inventory Control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections	L	L	L				
Provisional System Security Category			[redacted]				
Adjusted System Security Category			[redacted]				
Information System Security Impact Level							[redacted]

Adjust the Information Type's Provisional Impact Values

The information owner/information system owner reviews the appropriateness of the provisional security impact values for each security objective for each information type (i.e., the information type's security category) in the information system. The provisional impact values should be adjusted as necessary based on the special factors guidance provided for each information type. If adjusted, the rationale for the adjustment of an information type is documented in the system security plan.


•Updated system security plan with the system's provisional Impact values
•System description and mission
•Risk assessment results
Inputs
Adjust the Information Type's Provisional Impact Values
•Adjust the provisional impact values
•Document the adjusted security impact values in the security plan
•Updated system security plan with the adjusted impact values
•Rationale for adjustments
Outputs

Adjust the Provisional Impact Values

The information owner/information system owner reviews the appropriateness of the provisional security impact values for each information type by reviewing the rationale provided in NIST SP 800-60 or in the organization's supplement for the recommended security impact value for each security objective and the special factors affecting the impact value determination. The special factors guidance in NIST SP 800-60, Volume II, or the organization's supplement to NIST SP 800-60 provides specific guidance on how to adjust each security objective (confidentiality, integrity, and availability). The special factors guidance is applied to each information type based on how the information type is used, the organization's mission, interconnections with other systems, preliminary assessment of risk, or the system's operating environment. The information owner/information system owner determines if a change to a security impact value is warranted. In many cases, no change to the security category is necessary. If the security category is adjusted, the rationale for the adjustment is documented in the system security plan.

For example, information type C.2.3.4, *Strategic Planning*, has a recommended provisional impact value of *low*, but the special factors guidance states: "Unauthorized disclosure of some of the background information that supports development of some federal strategic plans can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be *moderate*, *high*, or involve *national security information* (outside the scope of this guideline)." The information owner/information system owner analyzes the information in their system to determine if it could reveal sensitive information, if so, the confidentiality impact level should be raised to *moderate*.

Document the Adjusted Impact Values

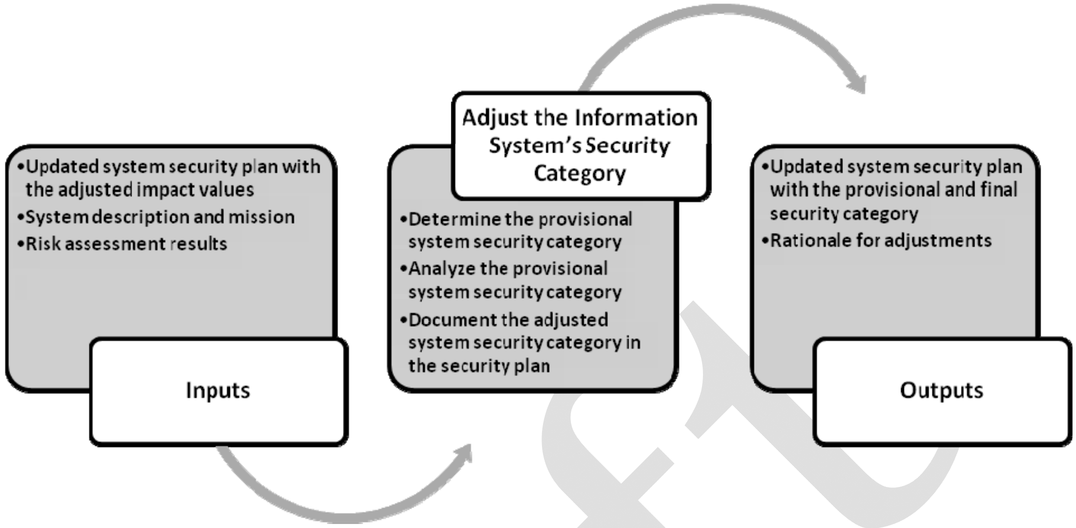
The adjusted impact values for each security objective are added to the information type table along with the supporting rationale to increase or decrease the values. If, after analyzing the provisional security category, the impact values did not change, the table should be updated to state *no adjustment needed*. The security category for the first adjusted information type is expressed as:

SC $_{\text{Corrective Action}}$ = {(confidentiality, low), (integrity, moderate), (availability, low)}

	Security Category						
Information Type Title, Reference, Description	Provisional			Final			
	C	I	A	C	I	A	Adjustment Rationale
Corrective Action, C.2.1.1, POAMs include information on non-compliant information systems within the organization	L	L	L	L	M	L	The impact value for the integrity impact value was increased to moderate to provide increased protection from unauthorized changes to the organization's POAMs and schedule of corrective actions to maintain the effectiveness of the organization's compliance program, per guidance in NIST SP 800-60.
Program Evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission. Per NIST SP 800-60, the confidentiality and integrity impact values should be commensurate with the impact levels of the system being evaluated.
Program Monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission.
Inventory Control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections	L	L	L	M	L	L	The list of the organization's information systems can be exploited to perpetrate fraud; therefore, the confidentiality impact value was increased to moderate.
Provisional System Security Category			[redacted]				
Adjusted System Security Category			[redacted]				
Information System Security Impact Level							[redacted]

Adjust the System's Provisional Security Category

After each information type has been adjusted, the provisional system security category is determined. The information owner/information system owner, with input from senior management, reviews the impact values for confidentiality, integrity, and availability to determine if they are applicable to the information system or if a more realistic view of the potential impact on the system requires increasing one or more security objectives of the security category. If the impact value of a security objective is changed, the final, adjusted system security category is documented in the system security plan along with the rationale for the change. The final system security category determines how an information system's security controls can be adjusted and reflects the most realistic expectations for each security objective so that appropriate decision can be made in the Select Step of the Risk Management Framework.


•Updated system security plan with the adjusted impact values
•System description and mission
•Risk assessment results
Inputs
Adjust the Information System's Security Category
•Determine the provisional system security category
•Analyze the provisional system security category
•Document the adjusted system security category in the security plan
•Updated system security plan with the provisional and final security category
•Rationale for adjustments
Outputs

Determine the Provisional System Security Category

After the impact values for each information type have been adjusted and documented in the system security plan, the information owner/information system owner determines the provisional system security category by considering the highest value assigned to each security objective (i.e., confidentiality, integrity, and availability) among the system's information types. Using the high water mark (highest value) for each security objective, the information owner/information system owner assigns the value of *low*, *moderate*, or *high*. In the above example, the confidentiality and integrity values for at least one information types was changed from *low* to *moderate*. Therefore, the highest value in the confidentiality and integrity columns is an M for *moderate*. The value for availability remained at *low*. The provisional system security category is expressed as:

SC $_{\text{EXAMPLE SYSTEM}}$ = {(confidentiality, moderate), (integrity, moderate), (availability, low)}

Analyze the System Security Category

After the provisional system security category has been determined, the information owner/information system owner determines if there is a need to increase the impact value of one or more of the security objectives based on a more realistic view of the potential impact a security breach could have on the information system. The information owner/information system owner considers factors such as aggregation of information, interconnections with other systems, protection of public information, loss of system availability, use of information within critical infrastructure or key national assets, preliminary assessment of risk, and other extenuating circumstances. Each security objective is reviewed from the system and organizational perspective instead of the perspective of an individual information type.

For example, the system's availability impact value in the provisional system security category may be *low*, but other systems may rely on the information to provide a critical function justifying an increase in the availability impact value to *moderate* or *high*. Senior management provide this perspective, moving beyond the impact on an individual information system to the impact on the organization and its ability to fulfill its mission and business goals.

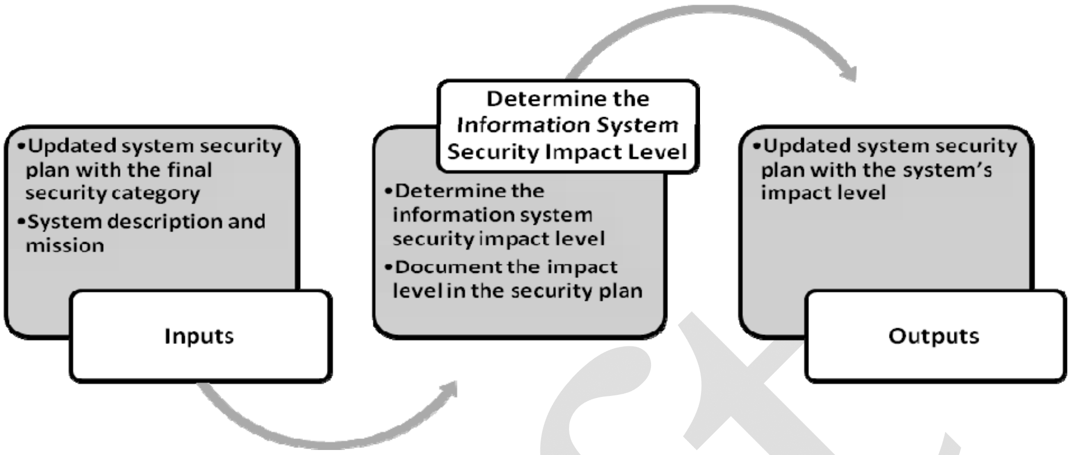
Document the Adjusted System Security Category

The final, adjusted system security category is documented in the system security plan along with the rationale for the decision. If, after analyzing the provisional system security category, the impact values for the security objectives do not change, the table is updated to state *no adjustment needed*. In this example, the impact value for availability was increased to *moderate* due to the number of organizational decision makers that depend on the information in this system.

Information Type Title, Reference, Description	Security Category						Adjustment Rationale
	Provisional			Final			
	C	I	A	C	I	A	
Corrective Action, C.2.1.1, POAMs include information on non-compliant information systems within the organization	L	L	L	L	M	L	The impact value for the integrity impact value was increased to moderate to provide increased protection from unauthorized changes to the organization's POAMs and schedule of corrective actions to maintain the effectiveness of the organization's compliance program, per guidance in NIST SP 800-60.
Program Evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission. Per NIST SP 800-60, the confidentiality and integrity impact values should be commensurate with the impact levels of the system being evaluated.
Program Monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission.
Inventory Control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections	L	L	L	M	L	L	The list of the organization's information systems can be exploited to perpetrate fraud; therefore, the confidentiality impact value was increased to moderate.
Provisional System Security Category			[redacted]	M	M	L	
Adjusted System Security Category			[redacted]	M	M	M	Senior leaders rely on the ready availability of up-to-date compliance data for decision making; therefore, availability is increased to moderate.
Information System Security Impact Level							[redacted]

DETERMINE THE INFORMATION SYSTEM SECURITY IMPACT LEVEL

After the provisional system security category has been determined, the information system's security impact level is determined (by using the high water mark of the system security category). The system's impact level is the highest impact value for any of the security objectives.


Determine the Information System Security Impact Level
•Updated system security plan with the final security category
•System description and mission
Inputs
•Determine the information system security impact level
•Document the impact level in the security plan
•Updated system security plan with the system's impact level
Outputs

Determine Information System Security Impact Level

After the system security category has been determined based on the high water mark of the adjusted information types, the information owner/information system owner determines the system's impact level. The impact level is the highest value assigned to a security objective in the system security category. In the example above, the highest impact value is *moderate*. Therefore, the system's impact level is *moderate*.

In another example, the system security category is:

$SC_{\text{EXAMPLE SYSTEM}}$ = {(confidentiality, high), (integrity, moderate), (availability, low)}

In this case, the system security impact level is *high* since high is the highest impact value of any of the security objectives in the example. While this system impact level indicates that the system starts with the high baseline of security controls, the security controls can be adjusted based on the three impact values of the security category during the Select Step of the Risk Management Framework.

Document the System's Impact Level

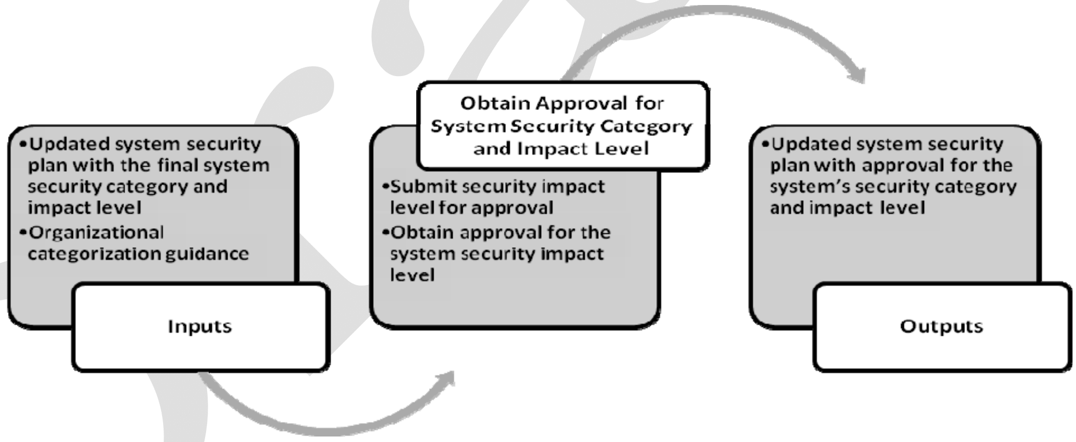
After the information owner/information system owner has determined the final system security impact level, the impact level is documented in the system security plan. In this example, the system's impact level is *moderate*.

Information Type Title, Reference, Description	Security Category						Adjustment Rationale
	Provisional			Final			
	C	I	A	C	I	A	
Corrective Action, C.2.1.1, POAMs include information on non-compliant information systems within the organization	L	L	L	L	M	L	The impact value for the integrity impact value was increased to moderate to provide increased protection from unauthorized changes to the organization's POAMs and schedule of corrective actions to maintain the effectiveness of the organization's compliance program, per guidance in NIST SP 800-60.
Program Evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission. Per NIST SP 800-60, the confidentiality and integrity impact values should be commensurate with the impact levels of the system being evaluated.

Program Monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)	L	L	L	M	M	L	The information system contains information on low- and moderate-impact systems that directly support the organization's mission.
Inventory Control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections	L	L	L	M	L	L	The list of the organization's information systems can be exploited to perpetrate fraud; therefore, the confidentiality impact value was increased to moderate.
Provisional System Security Category			■	M	M	L	
Adjusted System Security Category			■	M	M	M	Senior leaders rely on the ready availability of up-to-date compliance data for decision making; therefore, availability is increased to moderate.
Information System Security Impact Level			■	Moderate			[redacted]

OBTAIN APPROVAL FOR SYSTEM SECURITY CATEGORY AND IMPACT LEVEL

The information system's security impact level and security category should be approved as defined in the organization's categorization guidance before continuing to the Select Step in the Risk Management Framework. It is important to validate the categorization decision since this decision determines the selection of the security controls that will be implemented in the information system.


•Updated system security plan with the final system security category and impact level
•Organizational categorization guidance
Inputs
Obtain Approval for System Security Category and Impact Level
•Submit security impact level for approval
•Obtain approval for the system security impact level
•Updated system security plan with approval for the system's security category and impact level
Outputs

Submit System Security Impact Level for Approval

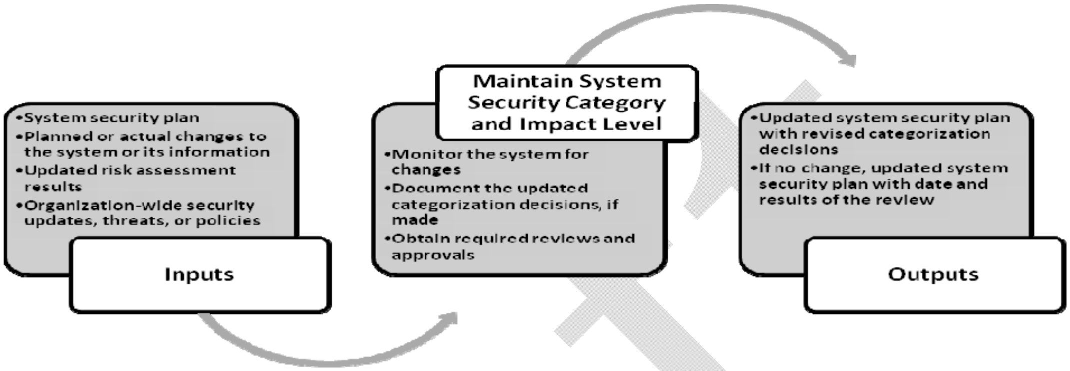
The information owner/information system owner submits the system security impact level, security category, and supporting rationale (e.g., the completed table above) to the appropriate organizational official who approves it and ensures its consistency with other organizational systems. Typically the system's impact level is approved by the authorizing official or the senior agency information security officer. The information owner/information system owner should be prepared to justify his or her determination of the kinds of information within the system, the selected information types, the adjusted security impact values for each information type, and the final security impact level.

Obtain Approval for the System Security Impact Level

The appropriate individuals, as designated in organizational categorization guidance, approve the system security impact level or work with the information owner/information system owner to adjust the final decision to make it more accurate and consistent with other systems within the organization. The system's impact level should be approved before the security controls are selected for the information system.

Maintain System Security Category and Impact Level

Periodically the information owner/information system owner reconfirms the criticality and sensitivity of the information system and the information processed, stored, or transmitted by the system to ensure that the system continues to support the organization’s mission or business case. Changes to the information system or its operating environment may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities.


•System security plan
•Planned or actual changes to the system or its information
•Updated risk assessment results
•Organization-wide security updates, threats, or policies
Inputs
Maintain System Security Category and Impact Level
•Monitor the system for changes
•Document the updated categorization decisions, if made
•Obtain required reviews and approvals
•Updated system security plan with revised categorization decisions
•If no change, updated system security plan with date and results of the review
Outputs

Monitor Information System for Changes

As part of the continuous monitoring process, the information owner/information system owner monitors the security controls in the information system. Changes or activities that could affect an information system include changes in the operating environment, new threats to the system, changes to the system functions, new interconnections, or added or removed information or information technology components. When changes to the information system have been identified, the information owner/information system owner determines the extent to which those changes and ongoing activities affect the system’s security impact level by analyzing the impact of the change on the system’s security posture.

Document Updated System Security Category

If the information system changes affect the system’s impact level, the system categorization effort should be reviewed and any resulting changes incorporated into the categorization documentation in the system security plan. If the system’s impact level changes, the related system documentation is updated. If the impact level increases, the information system owner implements any new security controls for the system in a timely manner.

Obtain Required Reviews and Approvals

If the system security impact level changes, the changes are updated in the system security plan and other related documentation. The information owner/information system owner is responsible for submitting the revised system security impact level to the appropriate organizational official for review and approval (or revision).

Categorize Step Summary

The information owner/information system owner is responsible for categorizing the information and information system and maintaining the categorization over the system’s life cycle. Following the guidance in NIST SP 800-60 and any organization-specific guidance, the information owner/information system owner prepares for the categorization process by obtaining appropriate documents and establishing relationships with other organizational entities affected by the categorization decision. To determine the information system’s security category and impact level, the information owner/ information system owner identifies the information types, selects the provisional or initial impact values (low, moderate, or high) for each security objective (confidentiality, integrity, and availability) for each information type, adjusts the security categories of the information types and identifies the system security category, adjusts the system security category for the information system, identifies the system's impact level, obtains approval for the system security category and impact level, and maintains the system's security category and impact level.

The results of the security categorization process are documented in the system security plan and includes the following:

- Information types for the information system
- Security category for each information type (consisting of three security impact values—one for each security objective of confidentiality, integrity, and availability)
- Security category for the information system
- Impact level for the information system derived from the system's security category (a single value of low, moderate, or high)
- Rationale for each of the adjustment decisions

REFERENCES

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I & II*, August 2008
- NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008
- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008
- Categorize FAQ, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/categorize/index.html